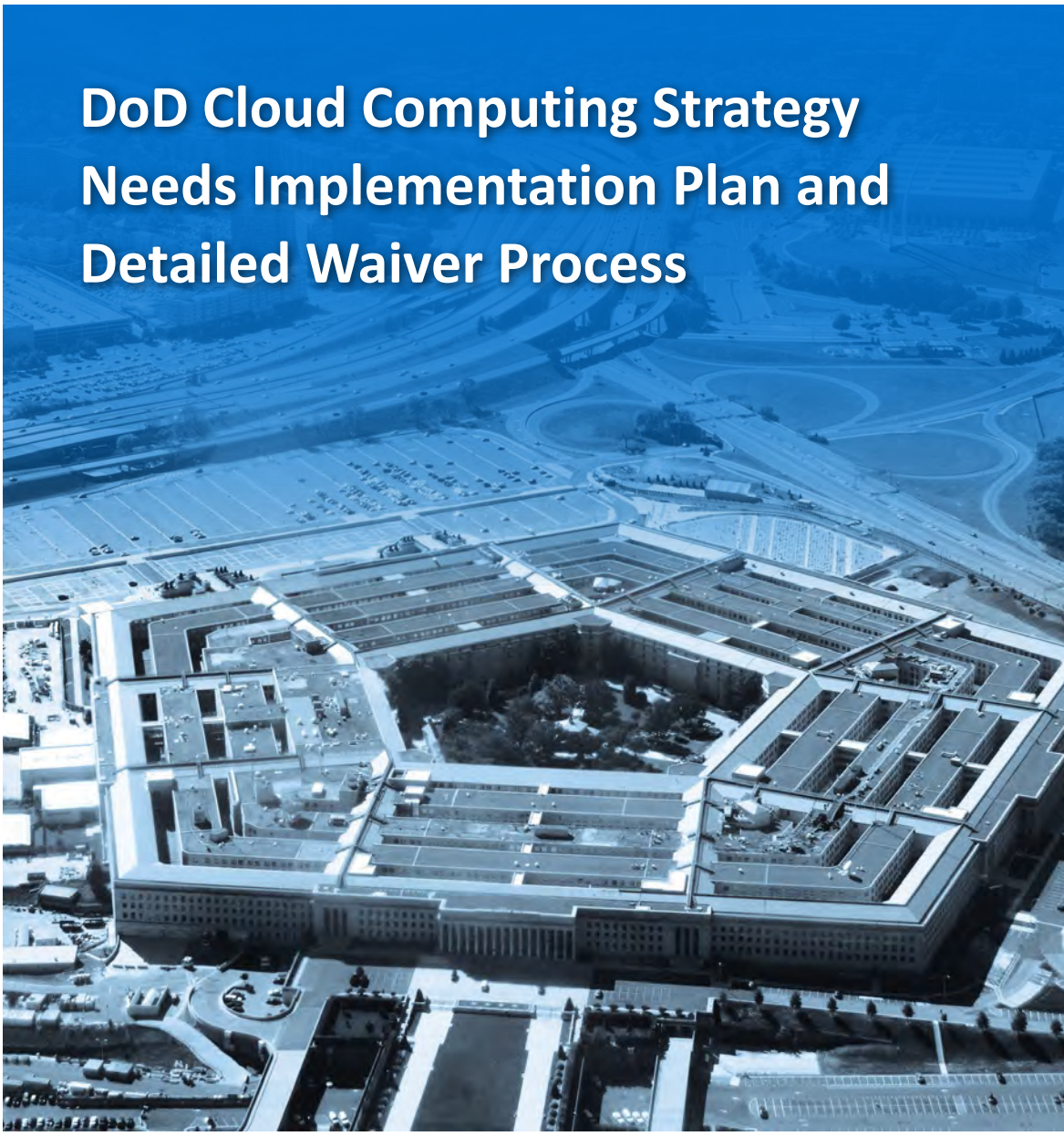
Report No. DODIG-2015-045

INSPECTOR GENERAL

U.S. Department of Defense

DECEMBER 4, 2014

DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
04 DEC 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense Inspector General,4800 Mark Center Drive,Alexandria,VA,22350-1500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**40**	

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline | 800.424.9098

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process

December 4, 2014

Objective

Our objective was to determine whether DoD effectively planned and executed a strategy for implementing cloud computing. This is the first in a series of audits on cloud computing.

Findings

DoD did not fully execute elements of the DoD Cloud Computing Strategy. For example, DoD did not fully develop skills training for the acquisition and contract specialists who procure cloud computing services and fully develop cloud service broker management capabilities.

For the three cloud computing contracts we reviewed, DoD Components did not obtain waivers from the designated review authority to use a non-DoD approved cloud service provider.

This occurred because the DoD Chief Information Officer did not develop an implementation plan that included assignment of roles and responsibilities and associated tasks, resources, and milestones. In addition, the DoD Chief Information Officer did not have a detailed written process for obtaining a cloud computing waiver.

As a result, DoD may not realize the full benefits of cloud computing. In addition, DoD was at greater risk of not preserving the security of DoD information against cyber threats.

Visit us at www.dodig.mil

Recommendations

Among other recommendations, we recommended that the DoD Chief Information Officer develop an implementation plan for the DoD Cloud Computing Strategy that assigns roles and responsibilities as well as associated tasks, resources, and milestones. We also recommended the Army Program Executive Officer Enterprise Information Systems and the Chief Information Officer, National Defense University work with the DoD Chief Information Officer and apply for waivers for their respective cloud computing contracts. Further, we recommend the DoD Chief Information Officer develop and publish a waiver process providing detailed guidance on how to obtain a cloud computing waiver.

Management Comments

The management comments received from the Acting Principal Deputy DoD Chief Information Officer, responding for the DoD Chief Information Officer, did not fully address our recommendation to develop an implementation plan for the DoD Cloud Computing Strategy, but did address our recommendation to develop and publish a cloud computing waiver process. In addition, the management comments received from the Army Project Director, Computer Hardware Enterprise Software and Solutions, responding for the Army Program Executive Officer Enterprise Information Systems, and Chief Information Officer, National Defense University addressed our recommendations to apply for waivers for their respective cloud computing contracts. We request that the DoD Chief Information Officer provide additional comments on the final report. Please see the Recommendations Table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
DoD Chief Information Officer	A	B.3
Army Program Executive Officer Enterprise Information Systems		B.1
Chief Information Officer, National Defense University		B.2

Please provide management comments by January 5, 2015.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

December 4, 2014

MEMORANDUM FOR DOD CHIEF INFORMATION OFFICER
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
PRESIDENT, NATIONAL DEFENSE UNIVERSITY

SUBJECT: DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process (DODIG-2015-045)

We are providing this report for your review and comment. The DoD Chief Information Officer issued a cloud computing strategy in July 2012, but did not develop a plan to implement the strategy to include assigning roles and responsibilities as well as associated tasks, resources, and milestones. In addition, DoD Components used non-DoD approved cloud service providers without obtaining a waiver from the DoD Chief Information Officer's designated review authority. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The comments from the Acting Principal Deputy DoD Chief Information Officer, responding for the DoD Chief Information Officer, did not address all aspects of Recommendation A. Therefore, we request that the DoD Chief Information Officer provide additional comments by January 5, 2015. The comments from the Army Project Director, Computer Hardware Enterprise Software and Solutions, responding for the Army Program Executive Officer Enterprise Information Systems, and Chief Information Officer, National Defense University addressed our recommendations and no additional comments are required.

Please provide comments that conform to the requirements of DoD Directive 7650.3. Please send a PDF file containing your comments to audrco@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 664-7331).

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

Contents

Contents (cont'd)

Management Comments


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Introduction

Objective

Our audit objective was to determine whether DoD effectively planned and executed a strategy for implementing cloud computing. This is the first in a series of audits we will perform on cloud computing. See Appendix A for a discussion of our scope and methodology.

Background

The National Institute of Standards and Technology defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of computing resources, such as networks and servers that can be quickly engaged with minimal management effort or service provider interaction. In December 2010, the Federal Chief Information Officer (CIO) issued the "25 Point Implementation Plan to Reform Federal Information Technology Management," which requires the Federal Government to shift to a "Cloud First" policy. According to the Federal CIO, the benefits of cloud computing include improved efficiency through better use of assets, reduced duplication, accelerated data center consolidation, increased service responsiveness, and innovation.

DoD Cloud Computing Strategy

In July 2012, the DoD CIO issued the DoD Cloud Computing Strategy to accelerate the DoD adoption of cloud computing and take advantage of its benefits. The strategy provides elements intended to foster adoption of cloud computing and establish a DoD cloud infrastructure. Elements in the strategy include, but are not limited to, the establishment of broker services, training, contract clauses, and broker management capabilities such as:

- providing an integrated billing and contracting interface;
- managing integrated service delivery from DoD and commercial cloud service providers (CSPs);
- controlling usage and optimizing cloud computing workload distribution; and
- providing a common, integrated helpdesk.

As part of implementing the DoD Cloud Computing Strategy, the DoD CIO issued a memorandum, "Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker," on June 26, 2012. This memorandum establishes the Defense Information Systems Agency (DISA) as the

DoD Enterprise Cloud Service Broker (ECSB) to provide a focal point to consolidate cloud service demand at the enterprise level and negotiate for the best service usage rates across DoD. The ECSB will leverage cloud services to increase secure information sharing and collaboration, enhance mission effectiveness, and decrease costs. The memorandum requires DoD Components to acquire cloud computing services through the ECSB or obtain a waiver from the DoD CIO designated review authority to ensure that security of DoD information is preserved. According to DoD CIO representatives, a waiver is primarily a mission-driven exception to DoD CIO requirements based on factors such as cybersecurity and efficiency.

Review of Internal Controls

DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, requires DoD Components to establish a program to review, assess, and report on the effectiveness of their internal controls. We identified internal control weaknesses in DoD's planning and execution of its strategy to implement cloud computing. Specifically, the DoD CIO did not develop a plan to implement the DoD Cloud Computing Strategy to include assigning roles and responsibilities as well as associated tasks, resources, and milestones and did not have a documented process providing detailed guidance on how to obtain a waiver for cloud computing services. We will provide a copy of this report to the senior official responsible for internal controls in the Office of the DoD CIO.

Finding A

DoD Cloud Computing Strategy Not Fully Executed

Although the DoD CIO issued a cloud computing strategy in July 2012, as of June 2014, elements of that strategy were not fully executed. For example, DoD did not fully develop specific skills training for the acquisition and contract specialists who procure cloud computing services and did not fully develop cloud service broker management capabilities. This occurred because the DoD CIO did not develop a plan to implement the cloud computing strategy to include assigning roles and responsibilities as well as associated tasks, resources, and milestones. As a result, DoD may not realize the full benefits of cloud computing such as cost savings, increased mission effectiveness, and increased cybersecurity.

Certain Strategy Elements Executed

The DoD CIO executed certain elements of the cloud computing strategy such as designating DISA as the ECSB and working to establish cloud computing contract clauses. For example, the DoD Cloud Computing Strategy stated that the DoD CIO was to work with the Under Secretary of Defense for Acquisition, Technology, and Logistics to modify or establish cloud computing contract clauses and make any accompanying changes necessary to the Defense Federal Acquisition Regulation Supplement. In response to that requirement, the Defense Procurement and Acquisition Policy initiated Defense Federal Acquisition Regulation Supplement Case 2013-D024, "Contracting for Cloud Services," in April 2013, to develop clauses to use when contracting for cloud services. According to Defense Procurement and Acquisition Policy representatives, the anticipated publication date for the clauses is September 2015. In the interim, the DoD CIO developed the "DoD Cloud Computing Contract Issues Matrix," December 16, 2013 (see Appendix B), for the acquisition and contract specialists to use when acquiring cloud services. The matrix contains 21 issues specific to cloud computing that should be addressed in cloud computing contracts. Although the DoD CIO executed certain elements of the DoD Cloud Computing Strategy, other elements were not fully executed. For example, DoD did not fully develop specific skills training for acquisition and contract specialists. DoD also did not fully develop cloud service broker management capabilities.

Skills Training Not Fully Developed

DoD did not fully develop skills training for the acquisition and contract specialists who procure cloud computing services. The DoD Cloud Computing Strategy stated that DoD was to provide specific skills training to acquisition and contracting specialists to facilitate acceptance and use of cloud computing technology. However, we confirmed with DoD CIO representatives that such training was not fully developed. In addition, DoD Component acquisition personnel indicated they were unsure of the specific steps in the DoD cloud computing acquisition process. According to DoD CIO representatives, DoD conducted contract training in June 2014 and DoD CIO representatives were working with the Defense Acquisition University to include cloud computing in acquisition courses. However, according to DoD CIO representatives, much of the training was on hold awaiting Defense Procurement and Acquisition Policy approval of the commercial cloud computing contract clauses. If the anticipated publication date for the clauses is September 2015, full development of the specific skills training could be postponed for at least another year.

In addition, DoD Component acquisition personnel indicated they were unsure of the specific steps in the DoD cloud computing acquisition process.

Cloud Service Broker Management Capabilities Not Fully Developed

Although the DoD CIO designated DISA as the DoD ECSB in June 2012, DoD did not fully develop cloud service broker management capabilities. According to the cloud computing strategy, the ECSB will provide capabilities such as:

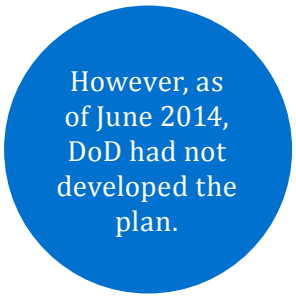
- providing an integrated billing and contracting interface,
- managing integrated service delivery from DoD and commercial CSPs,
- controlling usage and optimizing cloud computing workload distribution, and
- providing a common, integrated helpdesk.

The strategy indicates the ECSB would reduce duplicate efforts by providing those capabilities to all DoD Components, instead of each DoD Component having to provide its own. However, according to DoD CIO representatives, the ECSB has not yet implemented an enterprise contract for DoD approved commercial cloud

services. DoD CIO representatives stated that without an enterprise contract, there is no demand or ability to achieve these four capabilities. DoD CIO representatives anticipate that cloud service broker management capabilities will be extended to CSPs through future ECSB contract vehicles. However, ECSB representatives stated the ECSB was not yet providing those capabilities.

Implementation Plan Not Developed

DoD did not fully execute elements of its cloud computing strategy because the DoD CIO did not develop an implementation plan that assigned roles and responsibilities as well as associated tasks, resources, and milestones. According to the DoD CIO, an implementation plan was to follow the issuance of the DoD Cloud Computing Strategy and include further detail. However, as of June 2014, DoD had not developed the plan. According to DoD CIO representatives, they initially intended to develop a stand-alone plan for implementing a DoD cloud. However, since the Joint Information Environment (JIE)[1] was maturing and would cover much of the same material, DoD CIO representatives decided to include the cloud computing implementation in the JIE information and not develop a separate plan.



We requested that DoD CIO representatives provide the JIE implementation planning documentation that addressed tasks, resources, and milestones to implement selected elements of the cloud computing strategy. According to DoD CIO representatives, in February 2014, this information was included in the JIE Plan of Action and Milestones, which was being revised. In April 2014, DoD CIO representatives stated that the JIE Plan of Action and Milestones had been incorporated into the JIE Integrated Master Schedule, and included tasks and milestones to implement elements of the cloud computing strategy. However, DoD CIO could not provide a copy of the Master Schedule and could not otherwise show that roles and responsibilities for skills training and broker management capabilities were designated and that resources and milestones were assigned. For example, the cloud computing strategy states that skills training will be developed for acquisition specialists. However, the strategy does not specify who will develop the skills training or provide the associated milestones.

[1] The DoD Cloud Computing Strategy states the DoD cloud environment is a key component to enable the Department to achieve JIE success. According to DoD CIO Memorandum, "Joint Information Environment Implementation Guidance," September 26, 2013, the JIE is an effort to restructure the construction, operation, and defense of DoD information technology networks, systems and services to reduce costs and enhance mission effectiveness and cybersecurity.

Further, the strategy states the ECSB will provide specific cloud service management capabilities. However, the strategy does not provide associated milestones for the development of those capabilities. In addition, DoD CIO representatives cited the need to develop and implement a cybersecurity verification process and the need to modify the existing information technology infrastructure to support cloud as additional tasks that need to be accomplished. To help ensure the cloud computing strategy is implemented in a timely manner, DoD needs a mechanism to plan and prioritize efforts, monitor progress, and provide accountability through development of an implementation plan. Therefore, the DoD CIO should develop a plan to implement the DoD Cloud Computing Strategy that assigns roles and responsibilities and associated tasks, resources, and milestones for all unexecuted elements of the strategy.

DoD May Not Realize Full Benefits of Cloud Computing

By failing to execute all elements identified in the cloud computing strategy, DoD may not realize the full benefits of cloud computing, which include cost savings, increased mission effectiveness, and increased cybersecurity. DoD CIO developed the cloud computing strategy to accelerate the adoption of cloud computing in DoD. While the traditional delivery method of information technology focused on development, maintenance, and operation of computing hardware and software, the strategy states the cloud computing model focuses on providing information technology as a service. According to the cloud computing strategy, DoD will direct its efforts toward reducing reliance on non-shareable, dedicated infrastructures while increasing reliance on shared infrastructure through the use of cloud computing. Therefore, successful and accelerated execution of the cloud computing strategy can provide cost savings and increased cybersecurity through reduction in acquisition, operation, and maintenance of duplicative information technology hardware, software, and facilities. Further, the ability to rapidly provide cloud computing services in response to changes in DoD mission needs and to access DoD information when needed, regardless of location, will enhance mission effectiveness. The Federal CIO also cited benefits of cloud computing to include improved efficiency through better use of assets, reduced duplication, and accelerated data center consolidation, which would result in cost savings. In addition, the Federal CIO cited increased service responsiveness, which would result in increased mission effectiveness.

Further, the ability to rapidly provide cloud computing services in response to changes in DoD mission needs and to access DoD information when needed, regardless of location, will enhance mission effectiveness.

Management Comments on Finding A and Our Response

DoD CIO Comments

The Acting Principal Deputy DoD CIO, responding for the DoD CIO, disagreed that the strategy elements identified in Finding A hindered DoD's ability to realize the full benefits of cloud computing.

The Acting Principal Deputy stated the DoD CIO incorporated cloud computing implementation into the JIE Implementation Plan published in September 2013, rather than developing the plan in the July 2012 cloud strategy. He also stated that development of skills training for acquisition and contract specialists and the maturation of cloud broker management capabilities are evolving at a rate appropriate for DoD to address cybersecurity risks and integration challenges. With the development of the "DoD Cloud Way Ahead Report" and the cloud pilot programs underway, the Acting Principal Deputy said the necessary components are close to being in place. However, until these components are in place to address and mitigate cybersecurity risks, he said skills training and advanced cloud broker capabilities have minimal impact on DoD adoption of cloud computing.

The Acting Principal Deputy added that DoD identified contract issues in December 2013 and began offering cloud acquisition training in June 2014 and personnel are using that information to inform and guide acquisition efforts. Finally, he stated the DoD CIO is working with the Under Secretary of Defense for Acquisition, Technology, and Logistics to finalize and publish a Defense Federal Acquisition Regulation Supplement case on contracting for cloud services by September 2015.

Our Response

Although DoD is working to implement cloud computing, the DoD Cloud Computing Strategy has not been fully executed. Until it is, DoD may not achieve the full benefits of cloud computing cited by the strategy, such as cost savings and increased cybersecurity. We determined that at least two elements from the strategy—skills training for acquisition and contracting specialists and cloud service broker management capabilities—had not been fully executed. The Acting Principal Deputy stated DoD identified contract issues in December 2013 and began offering cloud acquisition training in June 2014. However, as cited in our report, DoD CIO representatives said much of the training was on hold,

awaiting Defense Procurement and Acquisition Policy approval of commercial cloud computing contract clauses; this approval is not expected until 2015. In addition, DoD CIO representatives said broker capabilities will not be needed until the ECSB implements an enterprise contract for DoD approved commercial cloud services. Further, DoD CIO representatives identified additional tasks that need to be done including modifying the existing information technology infrastructure to support cloud computing and developing and implementing a cybersecurity verification process.

We commend DoD for developing a "Cloud Way Ahead Report," initiating cloud pilot programs, identifying contract issues, offering acquisition training, and working to finalize and publish a Defense Federal Acquisition Regulation Supplement case on cloud contracting. However, as cited in our report, to help ensure the cloud computing strategy is implemented in a timely manner, DoD needs a mechanism to plan and prioritize efforts, monitor progress, and provide accountability through development of an implementation plan.

Recommendation, Management Comments, and Our Response

Recommendation A

We recommend the DoD Chief Information Officer develop a plan to implement the DoD Cloud Computing Strategy that assigns roles and responsibilities and associated tasks, resources, and milestones for all unexecuted elements of the strategy.

DoD CIO Comments

The Acting Principal Deputy, responding for the DoD CIO, partially agreed, stating adoption of the new overarching JIE incorporates the component of a cloud computing environment for DoD. He stated the JIE has an Integrated Master Schedule that assigns roles and responsibilities and associated tasks, resources, and milestones with the necessary elements of the strategy. He also stated the DoD CIO is developing DoD Instruction 8100.06, "Acquisition and Use of Externally Provided Cloud Services" with anticipated release by July 2015. In addition, he stated the DoD CIO and other DoD Components have developed a Cloud Acquisition Workshop, held twice in 2014, and additional sessions are planned. The Acting Principal Deputy also stated the DoD CIO is developing cloud computing updates for

the DoD Acquisition Guide for scheduled publication in August 2015, following the approval of DoD Instruction 8100.06. Finally, he stated the DoD CIO is supporting development of detailed cloud acquisition requirements in a Defense Federal Acquisition Regulation Supplement case expected to be released in September 2015.

Our Response

The response from the Acting Principal Deputy did not address all aspects of the recommendation. As cited in our report, DoD CIO could not provide a copy of the JIE Integrated Master Schedule and could not otherwise show that roles and responsibilities for skills training and broker management capabilities were designated and that resources and milestones were assigned. Although he cited a cloud workshop and provided milestones for development of a DoD instruction and updates to the Defense Acquisition Guidebook and Defense Federal Acquisition Regulation Supplement, the Acting Principal Deputy did not address all unexecuted elements of the strategy discussed in our report. Specifically, he did not provide DoD plans and milestones to:

- develop and provide the training that is on hold awaiting approval of commercial cloud computing contract clauses;
- implement enterprise contract vehicles for DoD approved commercial cloud services; and
- develop cloud service broker management capabilities.

Furthermore, he did not address the need to develop and implement a cybersecurity verification process and the need to modify the existing information technology infrastructure to support cloud as cited in our report. Therefore, we request the DoD CIO to provide additional comments on the final report.

Management Comments on Internal Controls and Our Response

DoD CIO Comments

The Acting Principal Deputy DoD CIO, responding for the DoD CIO, disagreed that weaknesses in the DoD CIO Internal Control Program hindered DoD's ability to realize the full benefits of cloud computing. The Acting Principal Deputy stated the DoD CIO Internal Control Program identified JIE as the strategy to close capability gaps, and the JIE strategy and concept has been approved by the Joint Chiefs of Staff. He also acknowledged that our report accurately identifies that the DoD

CIO did not deliver a document titled "DoD Cloud Implementation Plan." However, based on significant overlap between the implementation plan and the emerging JIE effort, the Acting Principal Deputy said the initial cloud implementation plan was incorporated into the JIE activities and plans.

Our Response

The Acting Principal Deputy stated the DoD CIO incorporated cloud computing implementation into the JIE Implementation Plan, published in September 2013, rather than developing the plan described in the July 2012 cloud strategy. However, as cited in our report, DoD CIO representatives said JIE implementation planning documentation was being revised. Furthermore, as cited in our report, DoD CIO representatives were not able to show (through JIE documentation or otherwise) that roles and responsibilities for skills training and broker management capabilities were designated and that resources and milestones were assigned.

Finding B

Waivers Not Obtained When Contracting With Non-DoD Approved Cloud Service Providers

For the three cloud computing contracts we reviewed, DoD Components did not obtain waivers from the DoD CIO designated review authority when contracting to use a non-DoD approved CSP. This occurred because the DoD CIO did not have a documented process detailing how to obtain a Global Information Grid (GIG)[2] waiver for cloud computing. As a result, DoD was at greater risk of not preserving the security of DoD information against cyber threats. Further, the DoD CIO did not know how the DoD information hosted on the cloud was protected and therefore could not assess the security risk to the GIG.

[2] The GIG includes all networks used for collecting, processing, storing, disseminating, and managing DoD information.

Waivers Not Obtained

For the three cloud computing contracts we reviewed, DoD Components contracted to use a non-DoD approved CSP but did not obtain a waiver from the DoD CIO designated review authority. In accordance with the DoD CIO memorandum, "Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker," June 26, 2012, DoD Components are required to acquire cloud computing services by using the ECSB or obtain a waiver from the DoD CIO designated review authority.[3] According to the DoD ECSB Cloud Security Model, Version 2.1, March 13, 2014, the ECSB provides a catalog of CSPs with a DoD provisional authorization approving the cloud service for use by DoD Components. According to DoD CIO representatives, a DoD provisional authorization certifies that DoD CIO cybersecurity requirements have been met for an information technology service, whereas a GIG waiver is primarily a mission-driven exception to DoD CIO requirements based on consideration of areas such as cybersecurity and efficiency. Therefore, DoD Components must either use a CSP with a DoD provisional authorization or obtain a GIG waiver. However, for the following three cloud computing contracts we reviewed, the Army Program Executive Officer Enterprise Information Systems[4] and National Defense University (NDU) used non-DoD approved CSPs and none of the contracts had a waiver.

[3] According to DoD CIO representatives, this is a GIG waiver obtained from the DoD Deputy CIO for Information Enterprise who is the DoD CIO designated review authority.

[4] The two Army contracts were blanket purchase agreements.

Table. Status of Cloud Computing Contracts Reviewed

DoD Component	Contract Number	Issue Date	Provisional Authorization	Waiver
Army	W52P1J-13-A-0014	Sep 24, 2013	No	No
Army	W52P1J-13-A-0015	Sep 27, 2013	No	No
NDU	SP4705-13-F-0015	Feb 22, 2013	No	No

To ensure adequate consideration of cybersecurity and efficiency, the Army Program Executive Officer Enterprise Information Systems and NDU should work with the DoD CIO and apply for waivers for the three cloud computing contracts we reviewed.

Documented Cloud Waiver Process Needed

Army Program Executive Officer Enterprise Information Systems and NDU did not obtain a GIG waiver for the three cloud computing contracts we reviewed because the DoD CIO did not have a documented waiver process for cloud computing. Although DoD cloud computing guidance requires DoD Components acquiring cloud services to obtain a GIG waiver if they do not acquire the cloud service through the ECSB, DoD cloud computing guidance does not provide the detailed steps needed to obtain the waiver. Other DoD guidance addresses the GIG waiver process but does not specifically cover cloud computing. For example, Chairman of the Joint Chiefs of Staff Instruction 6211.02D, "Defense Information Systems Network (DISN) Responsibilities," January 2012 and DISA's Defense Information Systems Network Connection Process Guide, November 2013, provide guidance on the DoD GIG waiver process, but do not specifically address cloud computing. The DoD CIO should develop and publish a waiver process providing detailed guidance on how to obtain a GIG waiver for cloud computing.

Although DoD cloud computing guidance requires DoD Components acquiring cloud services to obtain a GIG waiver if they do not acquire the cloud service through the ECSB, DoD cloud computing guidance does not provide the detailed steps needed to obtain the waiver.

Risk to DoD Information Increased While Risk to Global Information Grid Was Not Assessable

The use of non-DoD approved commercial cloud services without a GIG waiver increased the risk that DoD information could be compromised. Further, the DoD CIO did not know how DoD information hosted on the cloud was protected and

therefore could not assess the security risk to the GIG. We were not aware of any compromises of DoD information hosted by a commercial CSP. However, according to DoD CIO representatives, commercial cloud computing services were at risk of providing unauthorized access to DoD information because the information was placed outside of the DoD security perimeter. According to the DoD CIO, risk associated with the use of commercial cloud computing must be managed at the DoD enterprise level. Use of the GIG waiver process would provide visibility of the protection mechanisms for DoD information hosted by non-DoD approved commercial CSPs.

Management Comments on Finding B and Our Response

DoD CIO Comments

The Acting Principal Deputy DoD CIO, responding for the DoD CIO, disagreed that DoD Components did not obtain waivers because the DoD CIO did not have a documented process detailing how to obtain a GIG waiver for cloud computing. He stated the existing GIG waiver process is prescribed to obtain a cloud computing waiver, with DISA providing the first review of the waiver request. He said DoD Components were well informed of the requirement through DoD CIO memoranda, DoD Cloud Forums, and meetings. He added that DoD Components needed to follow the instructions in DoD CIO Memorandums "Interim Guidance Memorandum on Use of Commercial Cloud Computing Services," December 9, 2011, and "Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker," June 26, 2012. The Acting Principal Deputy stated the Broker was capable of supporting Component requirements through the GIG waiver process to successfully obtain a GIG waiver. Finally, although he disagreed that the weaknesses in the documentation led to the Components inability to obtain a waiver, the Acting Principal Deputy agreed the documentation can be improved.

Our Response

Neither memorandum cited by the Acting Principal Deputy provided the detailed steps needed to obtain the waiver. As cited in our report, DoD Component acquisition personnel indicated they were unsure of the specific steps in the DoD cloud computing acquisition process. In addition, DoD CIO representatives stated they were concerned that DoD Components did not understand the cloud computing acquisition process. Although the Acting Principal Deputy indicated the waiver process for cloud computing is the same as the existing GIG waiver

process, DoD CIO representatives said the existing waiver process focuses on system connections not used for cloud computing. As a result, the detailed steps for the process to obtain a waiver for cloud computing should be separate from the existing GIG waiver process.

Recommendations, Management Comments, and Our Response

Recommendation B.1

We recommend the Army Program Executive Officer Enterprise Information Systems work with the DoD Chief Information Officer and apply for Global Information Grid waivers for cloud computing contracts W52P1J-13-A-0014 and W52P1J-13-A-0015.

Army Program Executive Officer Enterprise Information Systems Comments

The Army Project Director, Computer Hardware Enterprise Software and Solutions, responding for the Army Program Executive Officer Enterprise Information Systems, agreed and said the Program Executive Office Enterprise Information Systems will work with the DoD CIO for a waiver for the two cloud computing contracts no later than the end of the second quarter of FY 2015.

Our Response

The response from the Army Project Director addressed all specifics of the recommendation, and no further comments are required.

Recommendation B.2

We recommend the Chief Information Officer, National Defense University work with the DoD Chief Information Officer and apply for a Global Information Grid waiver for cloud computing contract SP4705-13-F-0015.

NDU Comments

The NDU CIO agreed and said NDU would obtain a GIG waiver for the contract by December 2014.

Our Response

The response from the NDU CIO addressed all specifics of the recommendation, and no further comments are required.

Recommendation B.3

We recommend the DoD Chief Information Officer develop and publish a waiver process providing detailed guidance on how to obtain a Global Information Grid waiver for cloud computing in DoD.

DoD CIO Comments

The Acting Principal Deputy DoD CIO, responding for the DoD CIO, agreed and said the DoD CIO is creating a new DoD Instruction 8220.01, "DODIN Waiver Process," that will provide updated instructions for the waiver processes. The instruction is scheduled for publication in mid-2015.

Our Response

The response from the DoD CIO addressed all specifics of the recommendation, and no further comments are required.

Appendix A

Scope and Methodology

We conducted this performance audit from October 2013 through September 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We selected elements from the July 2012 DoD Cloud Computing Strategy for review and interviewed DoD CIO representatives to identify planning and execution of the strategy, such as development of formal implementation plans and the status of strategy execution. We interviewed representatives from DISA to identify their role and accomplishments, as the ECSB, in executing the DoD strategy. We also interviewed program managers and contracting officials about the Army and NDU use of commercial cloud computing. In addition, we coordinated with representatives from U.S. Cyber Command, Navy, Air Force, Defense Logistics Agency, and Defense Procurement and Acquisition Policy to clarify their involvement in DoD cloud computing activities. We reviewed key criteria related to implementing the DoD Cloud Computing Strategy, such as DoD CIO memorandums, "Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker," June 26, 2012 (the June 2012 DoD CIO memorandum), and "Supplemental Guidance for the Department of Defense's Acquisition and Secure Use of Commercial Cloud Services," December 16, 2013.

We requested information from DoD CIO representatives about DoD Components improperly using commercial cloud services. Based on the information received, we reviewed two Army blanket purchase agreements, one Air Force contract, two Navy contracts, and two NDU contracts. During our contract review, we determined one Navy contract and one NDU contract were not for cloud services. In addition, we determined the Air Force contract and the second Navy contract were awarded before the June 2012 DoD CIO memorandum requiring DoD Components to obtain cloud services through the ECSB or obtain a waiver. Therefore, we reviewed the two Army blanket purchase agreements, issued in September 2013, and one NDU contract, issued in February 2013, for adherence to the June 2012 DoD CIO memorandum.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Prior Coverage

We did not identify any prior audit coverage on DoD cloud computing over the past 5 years.

Appendix B

DoD Cloud Computing Contracts Issues

The matrix below provides cloud computing contracting issues cited by the DoD CIO in the memorandum, "Supplemental Guidance for the Department of Defense's Acquisition and Secure Use of Commercial Cloud Services," December 16, 2013.

DoD Cloud Computing Contracts Issues Matrix

#	Legal Rationale	Description of Issue	Applicable to:
1	Inspector General Act of 1978 Federal Information Security Management Act of 2002 (FISMA) NIST 800-53	PHYSICAL ACCESS The Agency needs to have physical access to a CSP data center to conduct inspections for FISMA, other audit purposes, or Inspector General investigations. These audits may be unannounced, so the Agency must ensure that its auditors have the access they need to complete their audits and investigations.	All Commercial Clouds
2	HSPD -12	PERSONNEL ACCESS In order to further protect DoD data, the Agency must require all CSP employees who have access to government data, architecture that supports government data, or any physical or logical devices/code be U.S. person per Executive Order 12333 and pass an appropriate background check as required by Homeland Security Presidential Directive -12.	All Commercial Clouds
3	Per the Freedom of Information Act (FOIA) case law unless there is a "consultant" relationship (see Department of Interior v Klamath) government information falls under the "release to one release to all" (see NARA v Favish) rule applies, which would prohibit the government from protecting information from the public if it was released to a contractor without an NDA. In addition 5 CFR 2635.703 prohibits Federal employees from releasing non-public information; a NDA is the equivalent for contractor personal.	NDA The Agency must require CSP employees with access to government data and other government confidential information to sign a non-disclosure agreement that would legally prevent a CSP employee from disclosing non-public government information.	All Commercial Clouds

DoD Cloud Computing Contracts Issues (cont'd)

DoD Cloud Computing Contracts Issues Matrix

4	Asset availability procedures	ASSET AVAILABILITY The Agency should ensure that the service level agreement with the CSP contains provision for asset availability. The level of asset availability will be determined by the Agency's requirements.	All Commercial Clouds
5	The banner language provides consent for government to view any content on the system without a warrant that would otherwise be required by the 4th Amendment. See also, City of Ontario v. Quon.	BANNER Banners or consent to monitor language allows Federal law enforcement the right to access and review government data including email created on a government system without a warrant or a subpoena. When a Government is only procuring hosting the banner will be a requirement of the government or contractor who developed the system, however, when the government procures software as a service, the Agency must require the CSP to display the Agency's approved banner language prior to allowing a user access to the system.	All Commercial Clouds
6	FAR 9.5 on Organizational Conflict of Interest prohibit a contractor from using information from its government work for other commercial needs.	ORAGANIZATIONAL CONFLICT OF INTEREST When the government places non-public information on a commercial cloud, the Agency must ensure the CSP refrains from using government data for any purpose other than expressly stated in the requirements.	When CUI will be hosted in the cloud
7	FISMA states that the Agency is responsible for accepting the risk for an IT system.	CONTINUOUS MONITORING FedRAMP has mandated certain requirements for continuous monitoring in the "Continuous Mentoring Strategy Guide". These requirements require the CSP to produce certain reports and provide them to FedRAMP PMO and/or the FedRAMP 3PAO. The government client needs to request copies of these reports in its requirements (PWS/SOW), as the DoD Designated Authorizing Authority (DAA) is ultimately responsible for the protection of the data.	All Commercial Clouds

DoD Cloud Computing Contracts Issues (cont'd)

DoD Cloud Computing Contracts Issues Matrix

8	Memorandum M-07-16, May 22, 2007, for safeguarding against and responding to breaches of PII; FISMA; requirements for agency incident response plans and reporting to the Federal information security incident center established by the Act, i.e., United States-Computer Emergency Readiness Team (US-CERT), within the Department of Homeland Security. See 44 U.S.C. 3544(b)(7), 3546. Applicable law and policy includes section 208 of the E-Government Act of 2002 (E-GOV Act), and Office of Management and Budget (OMB) Memorandum M-03-22.	DATA BREACH/PIA As with any IT system there is always a risk of a data breach. As such, the Agency must require the CSP to provide a plan for handling such a breach which includes the requirement to notify the Agency of a breach within 60 minutes (US Cert Requirement). In addition, the Agency is required to conduct a Privacy Impact Assessment (PIA) on all its IT systems. The purpose of the PIA is to analyze how information in identifiable form is handled: to ensure that its handling conforms to applicable legal, regulatory, and policy requirements for privacy; to determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system; and to examine and evaluate protections and alternative processes for handling such information to mitigate potential privacy risks. To assist the Agency in developing the PIA, the CSP must be required to provide the Agency with any required data about the CSP environment.	When CUI will be hosted in the cloud
9	Inspector General Act of 1978 FISMA	FACILITY INSPECTIONS FISMA and DoD policy require that facilities hosting DoD data meet certain security standards. Routine inspections ensure that facilities are in compliance with these standards. Usually these inspections are conducted by the government; however, in the case of a CSP the government may agree to allow a third party to conduct an inspection based on the government's criteria.	All Commercial Clouds
10	FISMA	COMPLIANCE It is important to remind CSP's that when hosting government data they must comply with the FISMA and subsequent Agency policies.	All Commercial Clouds

DoD Cloud Computing Contracts Issues (cont'd)

DoD Cloud Computing Contracts Issues Matrix

11	Common law theory of privity of contract. The government needs to be in contract with the host of the data.	USE OF SUBCONTRACTORS When subcontracting, the Agency should ensure the prime retains operational configuration and control of DoD data. This is particularly important in the event of a data breach.	All Commercial Clouds
12	Sovereign Immunity clause of the Constitution Article III Section II. The government has not granted immunity to be sued for actions by third parties. See also the Federal Torts Claim Act.	INDEMNIFICATION Indemnification by the CSP protects the government when third parties sue the government for a tort when the CSP, not the government was liable. Indemnification also allows the government to recoup any costs related to a third party law suit.	All Commercial Clouds
13	Liability insurance requirement.	INSURANCE The Agency must require a CSP to have the necessary insurance to pay for any costs stemming from a breach of DoD data or to replace any damages to the DoD system.	All Commercial Clouds
14	Sovereign Immunity under the Article III Section II of the Constitution. US Government data is sovereign and is not subject to other jurisdictions.	JURISDICTION DoD data can only be released by an authorized official or by a court order from a US Federal Court. If a CSP places DoD data in a foreign jurisdiction its servers would be subject to the laws of that jurisdiction and risks DoD data being seized by a foreign government.	All Commercial Clouds
15	Inspector General Act of 1978 FISMA Law Enforcement Authorities	LAW ENFORCEMENT As mentioned above, all users to DoD systems have consented through the banner language to monitoring of their use of a DoD system and use of that data for law enforcement purposes. As such, Federal law enforcement officials do not need a warrant or a subpoena to access government data on a government system.	All Commercial Clouds
16	This clause just discusses maintenance responsibilities.	MAINTANCE	All Commercial

DoD Cloud Computing Contracts Issues (cont'd)

DoD Cloud Computing Contracts Issues Matrix

		Agencies should require CSPs to conduct regular maintenance including patches on its environment to prevent intrusions.	Clouds
17	Sovereign Immunity under the Article III Section II of the Constitution. US Government data is sovereign and is not subject to other jurisdictions.	NOTIFICATION Similar to jurisdiction, CSP data centers are subject to state and local law enforcement officials, and state and local subpoenas. The Agency must ensure the CSP notifies the Agency of a warrant or a subpoena so that the Department of Justice can protect Agency data from release.	All Commercial Clouds
18	Federal Records Act Freedom of Information Act Federal Rules of Civil Procedure	RECORDS The Agency is required to maintain and produce records per the Federal Records Act, the Freedom of Information Act, and the Federal Rules of Civil Procedure. Records are kept based on the Agency's disposition schedule. The government should work with the CSP to ensure that all government records and CSP records about government data are kept in accordance with Agency record's schedules.	All Commercial Clouds
19	CNSS 1001	SPILLIAGE Occasionally, classified information spills over to an unclassified system. When this happens, the agency must ensure the CSP follows the procedures in CNSS 1001.	All Commercial Clouds
20	HSPD 23 and NSPD 54, NDAA 2011 Section 806, DoDI 5200	SUPPLY CHAIN The Agency must ensure CSPs exercise due diligence to use genuine hardware and software products that are free of malware.	When CUI will be hosted in the cloud
21		TERMS OF SERVICE Many commercial services have Terms of Service Agreements that contain clauses that the government cannot accept. Below are some examples:	All Commercial Clouds

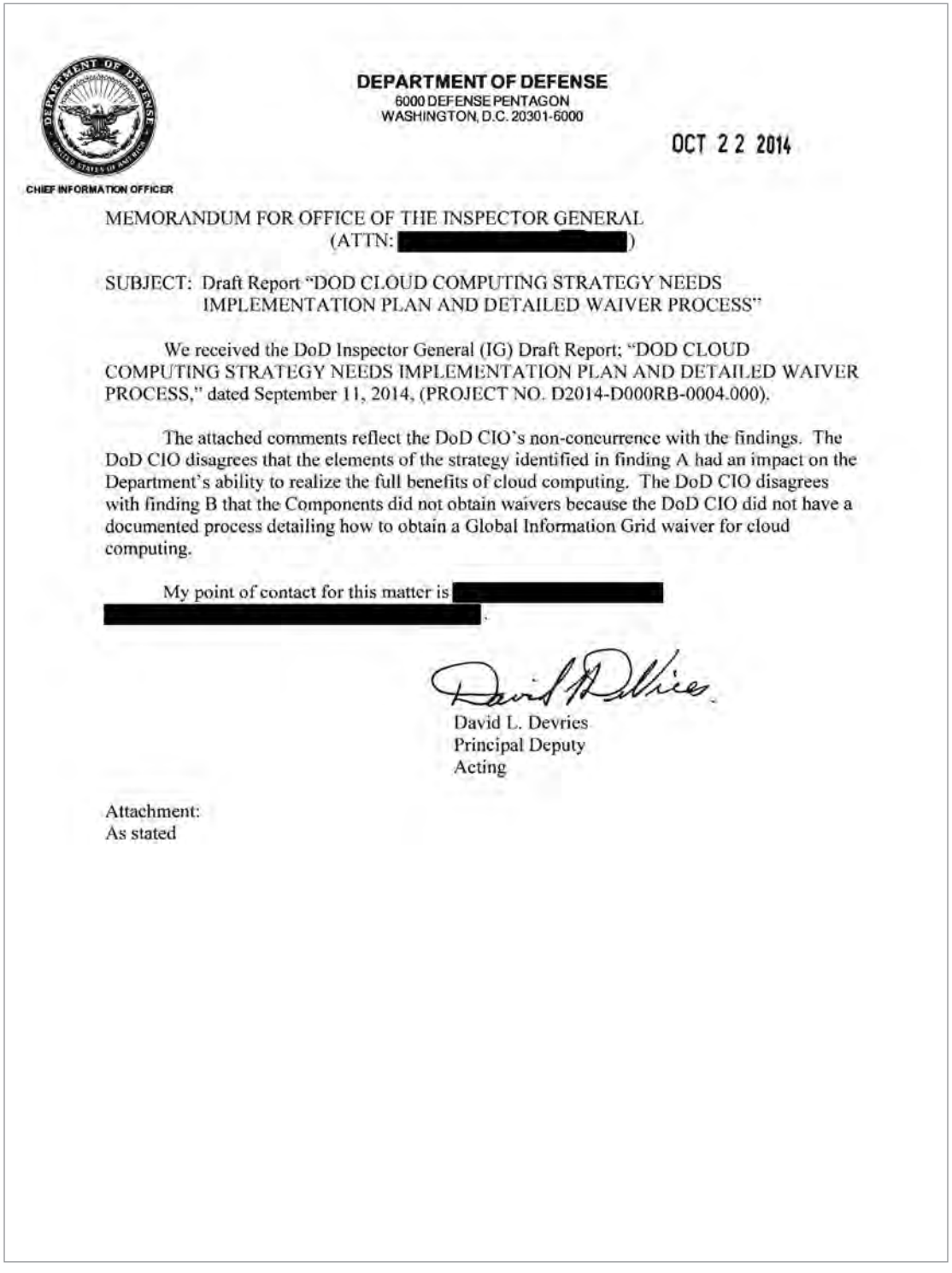
DoD Cloud Computing Contracts Issues (cont'd)

DoD Cloud Computing Contracts Issues Matrix

	Freedom of Information Act Article I Section 8 of the US Constitution. Congress has to appropriate money. Sovereign Immunity under the Article III Section II of the Constitution. US Government data is sovereign and is not subject to other jurisdictions. 5 C.F.R. 2635.702, the Federal Acquisition Regulation (FAR) (48 C.F.R. §3.101-1), Executive Order 12731	**CONFIDENTIALITY** This is a clause where the government agrees not to release confidential information. However, the government is subject to the Freedom of Information Act and must follow its procedures to release or protect commercial information. **INDEMNIFICATION** Many terms of service agreement contain an open ended indemnification clause where the government will indemnify the CSP against third party claims. This type of clause violates the Anti-Deficiency Act because the government is committing to funds that have yet to be appropriated. This clause needs to be re-worked to reference other applicable laws. **GOVERNING LAW** Many terms of service agreements have the governing law for the agreement to be a specific state and have a venue for any disputes to be in that state's courts. As the Federal government is not subject to state law, it can only be sued in Federal court. **ENDORSEMENT** Many terms of service agreements also have a clause where the CSP may quote / cite the government's use of its product as an endorsement or testimonial. The government does not endorse commercial products or services.	

Management Comments

DoD Chief Information Officer



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

OCT 22 2014

MEMORANDUM FOR OFFICE OF THE INSPECTOR GENERAL
(ATTN: [redacted])

SUBJECT: Draft Report "DOD CLOUD COMPUTING STRATEGY NEEDS IMPLEMENTATION PLAN AND DETAILED WAIVER PROCESS"

We received the DoD Inspector General (IG) Draft Report; "DOD CLOUD COMPUTING STRATEGY NEEDS IMPLEMENTATION PLAN AND DETAILED WAIVER PROCESS," dated September 11, 2014, (PROJECT NO. D2014-D000RB-0004.000).

The attached comments reflect the DoD CIO's non-concurrence with the findings. The DoD CIO disagrees that the elements of the strategy identified in finding A had an impact on the Department's ability to realize the full benefits of cloud computing. The DoD CIO disagrees with finding B that the Components did not obtain waivers because the DoD CIO did not have a documented process detailing how to obtain a Global Information Grid waiver for cloud computing.

My point of contact for this matter is [redacted].

David L. Devries
Principal Deputy
Acting

Attachment:
As stated

DoD Chief Information Officer (cont'd)

DOD IG DRAFT REPORT DATED SEPTEMBER 11, 2014
(PROJECT NO. D2014-D000RB-0004.000)

"DOD CLOUD COMPUTING STRATEGY NEEDS IMPLEMENTATION PLAN AND DETAILED WAIVER PROCESS"

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER COMMENTS TO THE DOD IG FINDINGS AND RECOMMENDATIONS

FINDING A: DOD CLOUD COMPUTING STRATEGY NOT FULLY EXECUTED

Although the DoD CIO issued a cloud computing strategy in July 2012, as of June 2014, elements of that strategy were not fully executed. For example, DoD did not fully develop specific skills training for the acquisition and contract specialists who procure cloud computing services and did not fully develop cloud service broker management capabilities. This occurred because the DoD CIO did not develop a plan to implement the cloud computing strategy to include assigning roles and responsibilities as well as associated tasks, resources, and milestones. As a result, DoD may not realize the full benefits of cloud computing such as cost savings, increased mission effectiveness, and increased cybersecurity.

DoD RESPONSE:

The DoD CIO disagrees that the elements of the Strategy identified in Finding A had an impact on the Department's ability to realize the full benefits of cloud computing. Cloud computing is evolving across the Federal landscape and within the Department driven by ever changing technology, industry service offerings and the ability to mitigate cyber threats. The DoD CIO realized that the full and robust implementation of a strategy will optimize DoD cloud computing. Therefore, the DoD CIO incorporated cloud computing implementation into the Joint Information Environment (JIE) Implementation Plan, published in September 2013, rather than developing the plan identified in the July 2012 Cloud Strategy.

As identified in the IG Report, the DoD CIO is developing skills training for acquisition and contract specialists, and maturing the Department's cloud broker management capabilities. These elements are evolving at a rate appropriate with our emerging ability to address the cybersecurity risks and integration challenges. The DoD CIO's efforts are heavily focused on addressing and mitigating the cybersecurity risks associated with outsourcing the Department's data and data processing to external cloud providers. With the development of the "DoD Cloud Way Ahead Report", and the cloud pilots that are currently underway, the necessary components are close to being in place. Until these components are in place, acquisition skills training and advanced cloud broker capabilities have minimal impact on the Department's adoption of cloud computing.

The DoD CIO disagrees with the finding that weaknesses in the DoD CIO's Internal Control Program (DODI 5010.40) contributed to the potential that DoD may not realize the full benefits of cloud computing. The DoD CIO's Internal Control Program identified the JIE as the Department's strategy to close 66 capability gaps identified in the GIG 2.0 Initial Capabilities Document (ICD), dated 29 May 2009, and the GIG 2.0 implementation guidance issued by the Deputy Secretary of Defense, dated 18 August 2011. The JIE strategy and concept was

DoD Chief Information Officer (cont'd)

approved by the Joint Chiefs of Staff on 6 August 2012. The Inspector General's report does accurately identify the fact that the DoD CIO did not deliver a document titled the "DoD Cloud Implementation Plan." However, based on significant overlap between the implementation plan and the emerging JIE effort, the initial Cloud Implementation Plan was incorporated into the JIE activities and plans.

As described above, evaluating and mitigating the cybersecurity risks have been the most significant challenge not just for the Department, but other Federal Agencies as well. Both the acquisition training and the cloud broker capabilities have matured at an appropriate rate that is synchronized with the Department's ability to actually begin outsourcing our data processing to commercial cloud providers. The Department identified cloud contract issues in December 2013 and began offering cloud acquisition training in June 2014. Acquisition and contacting officials are currently using that information to inform and guide acquisition efforts in anticipation of upcoming DoD Provisional Authorizations for use of commercial clouds at Levels 3-5. In addition, the DoD CIO is working with the Under Secretary of Defense for Acquisition, Technology, and Logistics to finalize and publish Defense Federal Acquisition Regulation Supplement Case 2013-D024, "Contracting for Cloud Services" by September 2015.

RECOMMENDATION A: *The DoD IG recommends the DoD Chief Information Officer develop a plan to implement the DoD Cloud Computing Strategy that assigns roles and responsibilities and associated tasks, resources, and milestones for all unexecuted elements of the strategy.*

DOD CIO RESPONSE: The DoD CIO partially agrees that elements of the DoD Cloud Computing Strategy have not yet been fully executed. As stated above, the evolving cybersecurity led to revision of the July 2012 strategy and adoption of the new overarching Joint Information Environment (JIE) that incorporates the component of a cloud computing environment for DoD. The JIE has an Integrated Master Schedule that assigns roles and responsibilities and associated tasks, resources, and milestones with the necessary elements of the strategy.

To improve the Department's acquisition of commercial cloud services, the DoD CIO is developing DoD Instruction 8100.06, *Acquisition and Use of Externally Provided Cloud Services.* This instruction will enter coordination in November 2014 with release anticipated by July 2015. To support acquisition training, the AF CIO, DISA, and the DoD CIO have developed a Cloud Acquisition Workshop for DoD contacting, legal and acquisition professionals. To date, this course has been held on two separate occasions: 18 June 2014 and 12 September 2014. In addition to offering additional workshop sessions, the DoD CIO is developing guidance for publication in the DoD Acquisition Guide (DAG). The cloud computing updates to the DAG are scheduled for publication in August 2015 following the approval of DoD Instruction 8100.06. The DoD CIO is also supporting the development of a Defense Federal Acquisition Regulation Supplement Case 2013-D024, "Contracting for Cloud Services," detailing cloud acquisition requirements. This DFAR clause is in the early stages of DoD Procurement and Acquisition Policy's (DPAP) DFAR rule making process. The DFAR clause is expected to be released by September 2015.

DoD Chief Information Officer (cont'd)

FINDING B: WAIVERS NOT OBTAINED WHEN CONTRACTING WITH NON-DOD APPROVED CLOUD SERVICE PROVIDERS

For the three cloud computing contracts the DoD IG reviewed, DoD Components did not obtain waivers from the DoD CIO designated review authority when contracting to use a non-DoD approved CSP. This occurred because the DoD CIO did not have a documented process detailing how to obtain a Global Information Grid (GIG)2 waiver for cloud computing. As a result, DoD was at greater risk of not preserving the security of DoD information against cyber threats. Further, the DoD CIO did not know how the DoD information hosted on the cloud was protected and therefore could not assess the security risk to the GIG.

DOD CIO RESPONSE:

The DoD CIO disagrees with Finding B that the Components did not obtain waivers because the DoD CIO did not have a documented process detailing how to obtain a GIG waiver for cloud computing. The existing GIG Waiver process is prescribed to obtain a cloud computing waiver. The waiver is a request for an exception to existing DoD policy -- primarily for connection to the GIG -- and it requires the same cybersecurity review and scrutiny as any other request. In this process, DISA provides the first review of the waiver request and makes a recommendation. The Components were well informed on the requirement through DoD CIO Memoranda, DoD Cloud Computing Forums and meetings.

Components needed to follow the instructions to obtain a GIG Waiver as stated in the DoD CIO Memorandum: "Interim Guidance Memorandum on Use of Commercial Cloud Computing Services," dated December 09, 2011, and contact the DoD Cloud Broker as described in the DoD CIO Memorandum: "Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker," dated June 26, 2012. The DoD Cloud Broker was capable of supporting a Component's requirement through the GIG Waiver Process. The Broker provides the direct support necessary to enter and execute the GIG Waiver Process. Components that contacted the Broker as required were able to successfully obtain a GIG Waiver.

While we disagree that weaknesses in the documentation led to the Components inability to obtain a waiver, the DoD CIO agrees that the documentation can be improved.

RECOMMENDATION B.3: *The DoD IG recommends the DoD Chief Information Officer develop and publish a waiver process providing detailed guidance on how to obtain a Global Information Grid waiver for cloud computing in DoD.*

DOD CIO RESPONSE: The DoD CIO agrees with the recommendation. The DoD CIO is currently creating a new DoD Instruction 8220.01, "DODIN Waiver Process," that will provide updated instructions for the waiver processes. The Instruction is scheduled for publication in mid-2015.

Department of the Army

DEPARTMENT OF THE ARMY
PROGRAM EXECUTIVE OFFICE
ENTERPRISE INFORMATION SYSTEMS
COMPUTER HARDWARE, ENTERPRISE SOFTWARE AND SOLUTIONS
9351 HALL ROAD
FORT BELVOIR, VA 22060

REPLY TO
ATTENTION OF

SFAE-PS-CH

15 Oct 14

MEMORANDUM FOR RECORD

SUBJECT: Draft Report "DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process (Project No. D2014-D000RB-0004.000)

1. PEO Enterprise Information Systems and Project Director Computer Hardware, Enterprise Software and Solutions concurs with the recommendation B1 in the Draft report dated September 11, 2014. PEO EIS will work with the DoD Chief Information Officer for a waiver for cloud computing contracts W52P1J-13-A-0014 and W52P1J-13-A-0015 no later than end of 2nd quarter FY 2015.

2. Point of Contact: [redacted].

3. Alternate Point of Contact: [redacted].

THOMAS W. NEFF,
Project Director
Computer Hardware
Enterprise Software and Solutions

National Defense University

THE JOINT STAFF
WASHINGTON, DC

14 October 2014

COMMENTS
DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process
D2014-D000RB-0004.000

NDU agrees with the findings and recommendations of the IG. NDU is moving forward to acquire any additional cloud computing services by using the ECSB or obtain a waiver from the DoD CIO designated review authority and, a GIG waiver for Google, by December 2014.

Stewart Liles, COL, USA
Chief Information Officer
National Defense University

Acronyms and Abbreviations

CIO	Chief Information Officer
CSP	Cloud Service Provider
DISA	Defense Information Systems Agency
ECSB	Enterprise Cloud Service Broker
GIG	Global Information Grid
JIE	Joint Information Environment
NDU	National Defense University

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

Monthly Update
dodigconnect-request@listserve.com

Reports Mailing List
dodig_report@listserve.com

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098